تكنولوجيا

تقنية توثيق بشرائح ذات بصمة مشتركة من دون خوادم خارجية

وداعاً لتخزين المفاتيح خارج الشريحة

أظهر النموذج الأولي تطابقاً في البصمة بنسبة تفوق 98 % ما يضمن توثيقاً مستقراً وموثوقاً (شاترستوك)

لندن: نسيم رمضان

نُشر: 19:14-26 فبراير 2026 م . 09 رَمضان 1447 هـ

في عالم الأمن السيبراني تقوم الثقة غالباً على أسرار مخزنة في مكان آخر؛ قد تكون على خادم أو داخل ذاكرة محمية أو في قاعدة بيانات سحابية. لكن ماذا لو لم يكن من الضروري أن تغادر هذه الأسرار الشريحة الإلكترونية أساساً؟

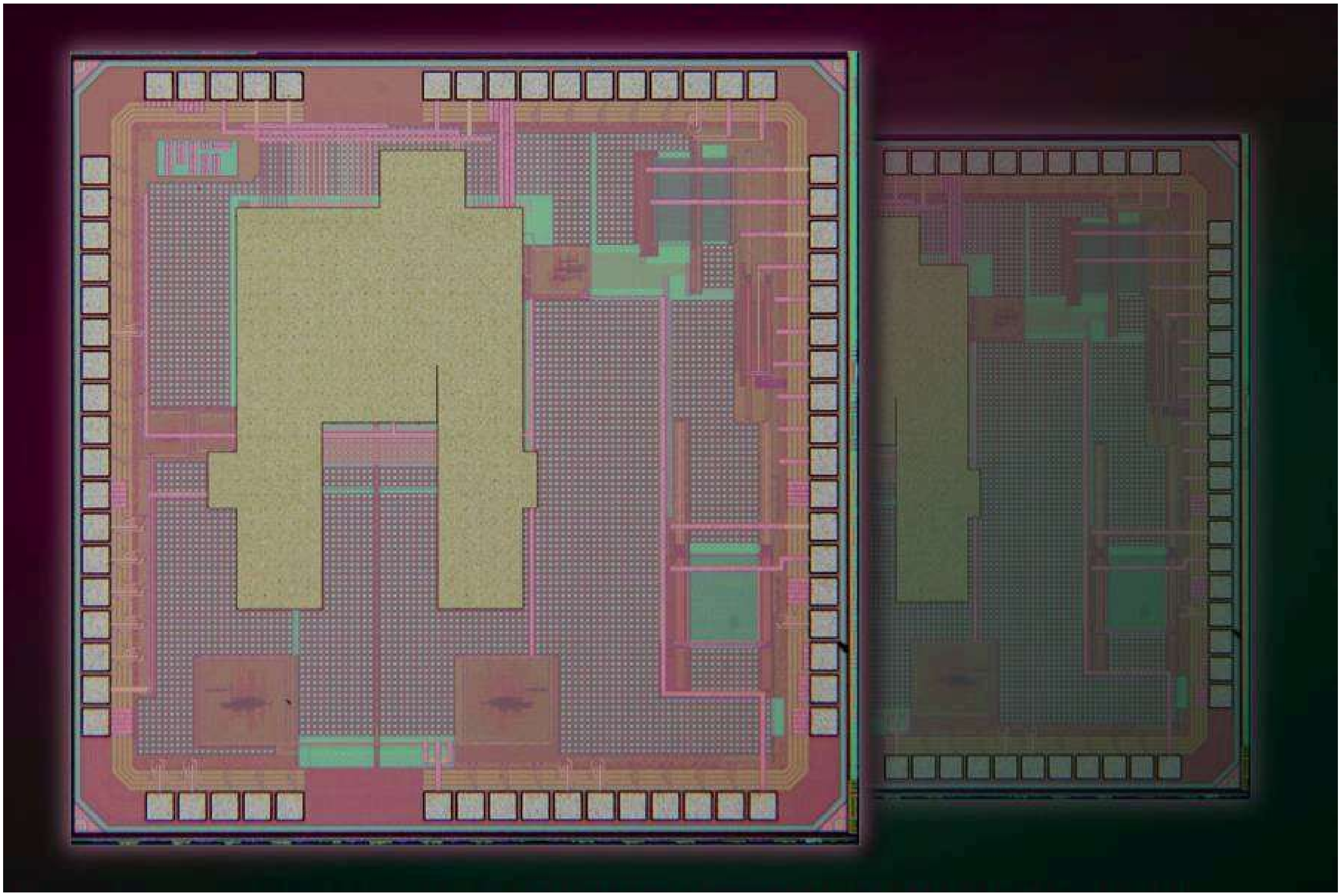
طوّر مهندسون في معهد ماساتشوستس للتكنولوجيا (MIT) تقنية تصنيع تُمكّن شريحتين إلكترونيتين من توثيق بعضهما عبر «بصمة» مادية مشتركة، من دون الحاجة إلى تخزين بيانات تعريف حساسة على خوادم طرف ثالث. ويمكن لهذه المقاربة أن تعزز الخصوصية وتخفض استهلاك الطاقة والذاكرة المرتبط عادةً بالأنظمة التشفيرية التقليدية.

الأسرار المخزّنة خارج الشريحة

حتى عندما تُصمَّم شرائح «CMOS» لتكون متطابقة، فإنها تحتوي على اختلافات مجهرية طفيفة تنشأ بشكل طبيعي أثناء عملية التصنيع. هذه الاختلافات تمنح كل شريحة توقيعاً مادياً فريداً يُعرف باسم «الدالة الفيزيائية غير القابلة للاستنساخ» (PUF). ومثل بصمة الإصبع البشرية، يمكن استخدام هذه الدالة للتحقق من الهوية.

في الأنظمة التقليدية، عندما يتلقى الجهاز طلب توثيق، فإنه يولّد استجابة تعتمد على بنيته الفيزيائية. ويقارن الخادم هذه الاستجابة بقيمة مرجعية مخزنة مسبقاً للتأكد من صحة الجهاز. لكن هذه البيانات المرجعية يجب أن تُخزَّن في مكانٍ ما، وغالباً على خادم خارجي. وإذا تم اختراق ذلك الخادم، تصبح منظومة التوثيق بأكملها عرضة للخطر.

يقول يون سوك لي، طالب الدراسات العليا في الهندسة الكهربائية وعلوم الحاسوب في «MIT» والمؤلف الرئيسي للدراسة: «أكبر ميزة في هذه الطريقة الأمنية أننا لا نحتاج إلى تخزين أي معلومات. ستبقى كل الأسرار داخل السيليكون دائماً».



تعتمد التقنية على استغلال الاختلافات المجهرية الطبيعية في تصنيع شرائح «CMOS» لإنشاء بصمة غير قابلة للاستنساخ (MIT)

شريحتان ببصمة واحدة

للتغلب على الاعتماد على التخزين الخارجي، ابتكر فريق «MIT» طريقة لتصنيع شريحتين تتشاركان بصمة مدمجة واحدة؛ أي بصمة فريدة لهاتين الشريحتين فقط.

ويمكن فهم الفكرة عبر تشبيه بسيط: تخيّل ورقة تم تمزيقها إلى نصفين، الحواف الممزقة عشوائية وفريدة، ولا يمكن إعادة إنتاجها بدقة. ومع ذلك، فإن القطعتين تتطابقان تماماً؛ لأنهما تتشاركان نفس الحافة غير المنتظمة. طبّق الباحثون هذا المفهوم أثناء تصنيع أشباه الموصلات؛ إذ تُنتج عدة شرائح في الوقت نفسه على رقاقة سيليكون واحدة قبل فصلها. واستغل الفريق هذه المرحلة لإدخال «عشوائية مشتركة» بين شريحتين متجاورتين قبل تقطيعهما. يشرح لي: «كان علينا إيجاد طريقة لتنفيذ ذلك قبل مغادرة الشريحة المصنع، لتعزيز الأمان. فبمجرد دخول الشريحة في سلسلة التوريد، لا نعرف ما الذي قد يحدث لها».

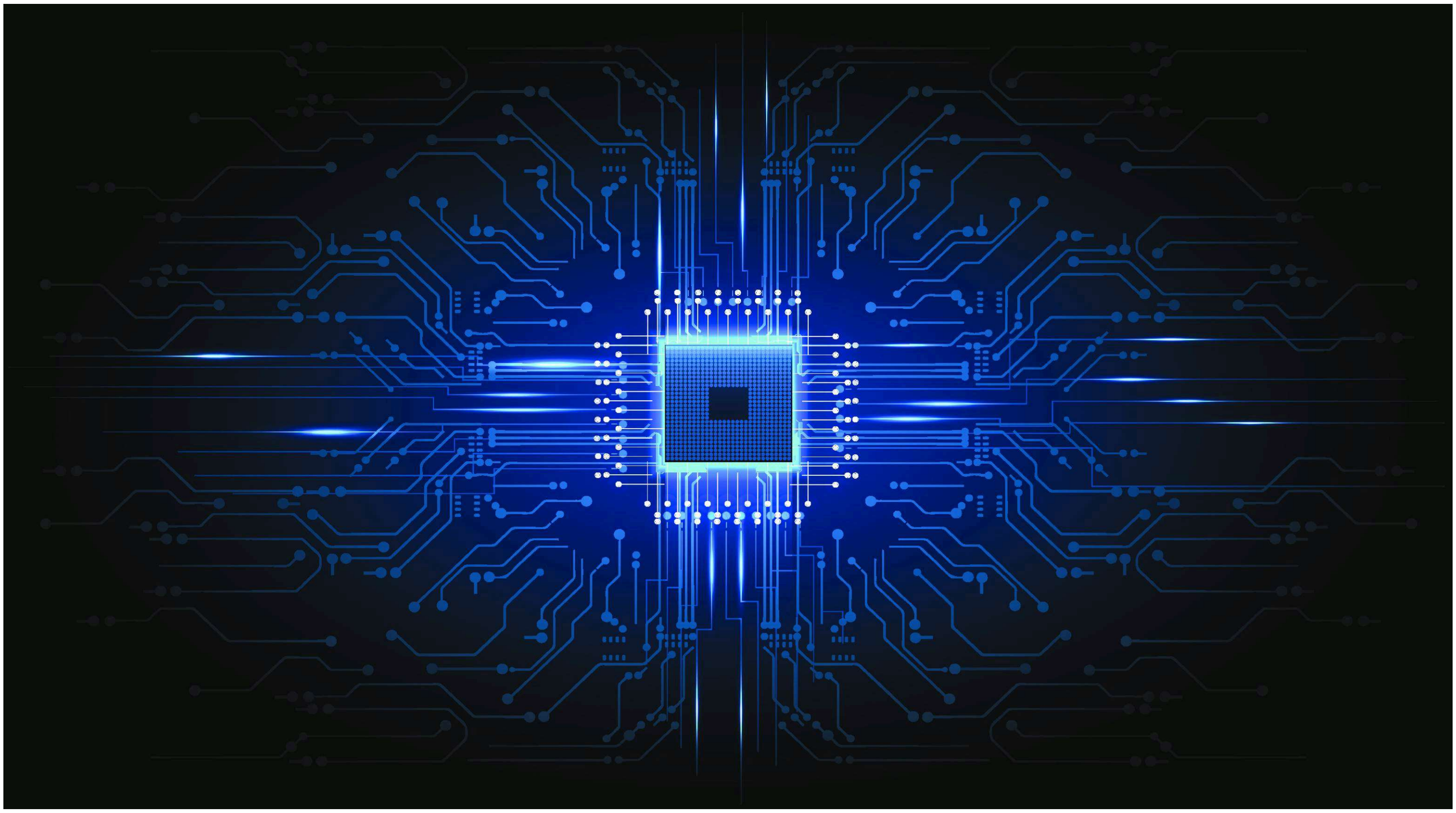
هندسة العشوائية داخل السيليكون

لإنشاء البصمة المشتركة، استخدم الباحثون عملية تُعرف باسم «انهيار أكسيد البوابة» (Gate Oxide Breakdown)؛ إذ يتم تطبيق جهد كهربائي مرتفع على ترانزستورات محددة مع تسليط ضوء «LED» منخفض التكلفة عليها. وبسبب الفروقات المجهرية الطبيعية، ينهار كل ترانزستور في لحظة مختلفة قليلاً. تمثل حالة الانهيار هذه مصدر العشوائية التي تُبنى عليها البصمة الفيزيائية.

ولإنشاء بصمة مزدوجة، صمّم الفريق أزواجاً من الترانزستورات تمتد عبر شريحتين متجاورتين، مع ربطها بطبقات معدنية أثناء وجودها على الرقاقة نفسها. وعند حدوث الانهيار، تتطور خصائص كهربائية مترابطة بين الترانزستورات المرتبطة.

بعد ذلك، تُقطَّع الرقاقة بحيث تحصل كل شريحة على نصف زوج الترانزستورات، وبالتالي تحتفظ كل واحدة ببصمة مشتركة مع الأخرى. وبعد تحسين العملية، تمكّن الباحثون من إنتاج نموذج أولي لشريحتين متطابقتين أظهرتا تطابقاً في العشوائية بنسبة تفوق 98 في المائة، وهي نسبة كافية لضمان توثيق مستقر وآمن.

ويقول لي إنه «لم يتم نمذجة انهيار الترانزستورات بدقة في العديد من المحاكاة، لذلك كان هناك قدر كبير من عدم اليقين. تحديد جميع الخطوات وتسلسلها لإنتاج هذه العشوائية المشتركة هو جوهر الابتكار في هذا العمل». والأهم أن التقنية متوافقة مع عمليات تصنيع «CMOS» القياسية، ولا تتطلب مواد خاصة. كما أن استخدام مصابيح «LED» منخفضة التكلفة وتقنيات دوائر تقليدية يجعل تطبيقها على نطاق واسع أمراً عملياً.



يمكن أن تفيد التقنية الأجهزة منخفضة الطاقة مثل المستشعرات الطبية عبر توفير أمن أعلى بتكلفة طاقة أقل (شاترستوك)

أهمية خاصة للأجهزة منخفضة الطاقة

يمكن أن تكون هذه التقنية مفيدة بشكل خاص في الأنظمة التي تعمل بقيود طاقة صارمة؛ إذ تُعد الكفاءة والأمن أولوية في آن واحد. فعلى سبيل المثال، قد تستفيد كبسولات استشعار طبية قابلة للبلع متصلة برقعة تُرتدى على الجسم من هذا النهج؛ إذ يمكن للكبسولة والرقعة توثيق بعضهما مباشرة من دون الحاجة إلى خادم وسيط أو بروتوكولات تشفير معقدة تستهلك طاقة إضافية.

يعد أنانثا تشاندراكاسان، نائب رئيس «MIT» والمؤلف المشارك في الدراسة، أن «هناك طلباً متزايداً بسرعة على أمن الطبقة الفيزيائية للأجهزة الطرفية». ويضيف أن منهج البصمة المزدوجة «يتيح اتصالاً آمناً بين العقد من دون عبء بروتوكولات ثقيلة، ما يحقق كفاءة في الطاقة وأمناً قوياً في الوقت نفسه».

نحو ترسيخ الثقة في العتاد نفسه

لا يقتصر البحث على الحلول الرقمية فقط؛ إذ يستكشف الفريق أيضاً إمكان تطوير أشكال أكثر تعقيداً من «السرية المشتركة» تعتمد على خصائص تماثلية يمكن تكرارها مرة واحدة فقط.

ويرى روانان هان، أستاذ الهندسة الكهربائية وعلوم الحاسوب والمؤلف المشارك في الدراسة، أن هذه الخطوة تمثل محاولة أولية لتقليل المفاضلة بين الأمان وسهولة الاستخدام. ويقول: «إن إنشاء مفاتيح تشفير مشتركة داخل مصانع أشباه الموصلات الموثوقة قد يساعد على كسر المفاضلة بين تعزيز الأمان وتسهيل حماية نقل البيانات».

ومع تزايد انتشار الأجهزة المتصلة وتوسع الحوسبة الطرفية، قد يصبح دمج الثقة مباشرة في العتاد أمراً ضرورياً. فمن خلال ضمان بقاء الأسرار داخل السيليكون نفسه، تشير هذه التقنية إلى مستقبل يُبنى فيه التوثيق داخل الشريحة لا خارجها.

مواضيع

تقنيات الذكاء الاصطناعي | تقنيات جديدة | تقنية | تكنولوجيا | الذكاء الاصطناعي | السعودية | أميركا